UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, vs. SERGEYI BAZAR, Defendant.	Case No.: 15-CR-499-BEN **ORDER DENYING MOTION TO SUPPRESS DIGITAL EVIDENCE**

Now before the Court is Defendant's motion to suppress digital evidence (filed September 9, 2015). The motion is denied.

Defendant seeks to suppress all digital evidence discovered through government searches of three Google accounts, a Facebook account, a Dell laptop computer, four cell phones and an Apple iPad. Defendant has not identified any particular evidence. And the motion is not based on the defendant's testimony or declaration of ownership or expectation of privacy in any of the accounts or devices. All of the accounts and devices were searched pursuant to search warrants issued by United States Magistrate Judge Nita L. Stormes or United States Magistrate Judge William V. Gallo.

Google and Facebook Accounts

As a preliminary matter, the defendant does not formally claim ownership of the three Google accounts named in the search warrants. Instead, the motion refers to the accounts as "three email accounts associated with Mr. Bazar." Neither does the defendant formally assert a reasonable expectation of privacy in the digital information. Similarly, for the Facebook account, the defendant does not formally claim ownership of the account nor does he assert that he has a reasonable expectation of privacy in the information on the Facebook page. Instead the motion refers to the Facebook account as "the account associated with Mr. Bazar."

While it is common experience that email accounts may be password protected, they may also be shared, while Facebook accounts are to various degrees open to viewing by anyone with an internet connection. Both types of digital accounts are probably viewable by employees of Google, Inc. and Facebook, Inc. which offer the accounts freely to the public. Consequently, the defendant has not made out a case for suppressing evidence from these sources even if no warrants had issued (in other words, he has not established "standing" in the Fourth Amendment sense), and the defendant has cited no case requiring suppression. *See United States v. Singleton*, 987 F.2d 1444, 1449 (9th Cir. 1993) (demonstration of a legitimate expectation of privacy is a threshold standing requirement that must first be established to seek suppression); *United States v. Azano Matsura*, No. 14CR388-MMA, 2015 WL 5449912, at *3 (S.D. Cal. Sept. 11, 2015) (describing the Fourth Amendment standing rule of *Alderman v. United States*, 394 U.S. 165, 175 n.9 (1969), that suppression of evidence from a Fourth Amendment violation can be urged only by those whose rights were violated by the search itself); *c.f. Sams v. Yahoo! Inc.*, 713 F.3d 1175, 1180 (9th Cir. 2013) (even 18 U.S.C. § 2703(c)(2) permits government to obtain basic subscriber information with a mere subpoena).

Assuming for the sake of argument that the defendant had carried his burden of demonstrating through evidence that he did have a reasonable expectation of privacy in the digital accounts, his motion fails because the searches were carried out on the

authority of valid search warrants. The warrants were supported by probable cause and were not overbroad or lacking in specificity. *C.f. United States v. Rudtke*, No. 11cr4956 WQH, 2014 WL 688800 (S.D. Cal. Feb. 20, 2014) (finding no reason to suppress Yahoo.com email information obtained through probable-cause-based search warrant that limited search to evidence related to federal crime charged).

Dell Laptop Computer

The Court has already held that the Dell laptop computer evidence was not subject to suppression. There is no reason to depart from that ruling. Moreover, the search was performed based upon a search warrant which was itself based on probable cause and sufficiently specific.

Apple iPad and Four Cell Phones

The defendant also seeks to suppress evidence obtained from an Apple iPad and four cell phones. The defendant does not formally claim ownership of the iPad or the four cell phones described in the search warrants. Neither does the defendant formally assert a reasonable expectation of privacy in the devices or digital information. He offers no testimony or declaration in support of his motion (for purposes of standing) and as a result fails to lay the requisite evidentiary foundation for a suppression motion.

Assuming the defendant could establish standing, his motion would still fail. According to the application for the search warrant, the defendant was arrested in an automobile. When he was arrested, he consented to a search of the automobile. The search of the automobile uncovered the iPad and the four cell phones. A search warrant for the content of these devices was then obtained from the Magistrate Judge. The defendant now argues an absence of probable cause to support the search warrant. But that argument is not convincing. The foundational evidence (*i.e.*, that the defendant used computer connections to advertise and cell phone text messages to entice, manage, and coerce victims into acts of sex-for-hire) is fully described in the applications for the search warrants. The facts described in the applications satisfy the probable cause requirement. *United States v. Kelly*, 482 F.3d 1047, 1050 (9th Cir. 2006) (en banc), *cert.*

denied, 552 U.S. 1104 (2008) (probable cause to search a computer turns on the totality of circumstances described and reasonable inferences).

The defendant also argues that the search warrant lacked specificity. But in the world of digital evidence, file names can be changed to suggest innocent information while hiding evidence of criminal activity. As a result, it is difficult to limit the breadth of a digital memory search where, as here, both written communications and images between numerous parties may contain evidence of the alleged crime. Some overbreadth is permissible. *United States v. Adjani*, 452 F.3d 1140, 1149-50 (9th Cir. 2006) ("To require such a pinpointed computer search, restricting the search to an email program or to specific search terms, would likely have failed to cast a sufficiently wide net to capture the evidence sought."); *see also United States v. Schesso*, 730 F.3d 1040, 1047-51 (9th Cir. 2013) ("The government was faced with the challenge of searching for digital data that was not limited to a specific, known file or set of files. The government had no way of knowing which or how many illicit files there might be or where they might be stored, or of describing the items to be seized in a more precise manner."); *United States v. Garcia-Alvarez*, 2015 WL 777411 (S.D. Cal. Feb. 24, 2015) ("Although it may have been better if the warrant had included a search protocol that minimized unnecessary intrusion into Defendant's personal data, here, as in *Hill* and *Schesso*, the absence of such a protocol did not render the warrant constitutionally defective, and agents were entitled to rely on it."); *United States v. Nazemzadeh*, 2013 WL 544054 (S.D. Cal. Feb. 12, 2013) ("Computer records are extremely susceptible to tampering, hiding, or destruction, whether deliberate or inadvertent. They are easy to disguise or rename, and were we to limit the warrant to such a specific search protocol, much evidence could escape discovery simply because of Nazemzadeh's labeling of the files documenting his criminal activity."). B*ut see United States v. Winn*, 79 F. Supp. 3d 904 (S.D. Ill. 2015), *appeal pending*, No. 15-1500 (7th Cir. Mar. 9, 2015) (suspected crime of public indecency did not require searching past photos and videos). The search warrant was not fatally overbroad or lacking in specificity.

Finally, assuming for the sake of argument that the defendant carried his burden of demonstrating standing to challenge the evidence, and assuming that either probable cause was lacking or that the search warrant was fatally overbroad and lacking in specificity, the good faith exception to the exclusionary rule would apply. "The fact that a Fourth Amendment violation occurred – *i.e.*, that a search or arrest was unreasonable – does not necessarily mean that the exclusionary rule applies." *Herring v. United States*, 555 U.S. 135, 140 (2009). "[E]vidence should be suppressed 'only if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth amendment.'" *Schesso*, 730 F.3d at 1050-51 (quoting *Herring*, 555 U.S. at 143). The "good faith" inquiry is confined to the question "whether a reasonably well trained officer would have known that the search was illegal in light of all the circumstances." *Herring*, 555 U.S. at 145 (quoting *United States v. Leon*, 468 U.S. 897, 922, n.23 (1984)). Because a reasonably well-trained officer would not have known that searching the defendant's iPad and cell phones was illegal based on the reasonable search warrant in-hand, the good faith exception applies. Because the good faith exception applies, the exclusionary rule does not apply. Therefore, the motion to suppress is denied.

Dated: October 21, 2015

Hon. Roger T. Benitez
United States District Judge